



Real-time Infrastructure Management: the Missing Link in Configuration Management Databases

Author: Kevin Gleason, Technical Manager CommScope Government Solutions

The sophisticated Network Centric Warfare (NCW) platforms – the sensors, weapons, logistics and command and control infrastructure, upon which today's modern militaries rely for superiority in the physical battle-space – depend on real-time situational awareness of the network cyberspace to be effective. Situational awareness in the network enables the warfighter to make better and faster decisions with confidence, knowing they have access to the best and most accurate information at their fingertips. Just as real-time awareness allows the soldier in the field to quickly turn information into actionable knowledge, enabling a measured response to a dynamic environment, real-time situational awareness of the network physical layer and its connected devices enable the rapid and measured response to network threats. This capability represents a significant enhancement to information assurance.

For NCW to succeed, the advantage of situational awareness and information assurance has to be realized both at the edge (warfighter) as well as the network core. As the warfighter relies on battle space awareness, the IT manager needs real-time situational awareness of their network to be able to ultimately support the NCW mission.

As these networks have become more complex, the need to understand both their capabilities as well as their vulnerabilities is clear. In response to this need, the federal government passed the Federal Information Security Management Act of 2002 (FISMA) that issues mandatory guidelines and reporting to provide a framework for protecting information and information systems. FISMA requires the chief information officer of the organization to develop and maintain an agency-wide Information Assurance (IA) program, as well as audit and report annually on its effectiveness; coordinate procedures to detect and respond to security breaches; and ready plans for continuity of operations.

In response, the U.S. Department of Defense has several initiatives to implement Information Technology Infrastructure Library (ITIL) framework in response to this regulatory requirement. The ITIL captures the Enterprise Architecture (EA) and IT best-practice processes, successfully used in the private sector for many years. ITIL serves as the basis for the new ISO/IEC 20000 standard.

A key component to ITIL is the Configuration Management Database (CMDB). While serving the central configuration repository, the CMDB keeps track of

Configuration Items (CI). The CIs tracked are network infrastructure components and associated assets – physical (equipment), logical (services) and service-level agreements. Although CMDB has been around for some time, the concept of a federated design offering real-time updates on configuration across the entire network and allied networks are not. A federated design allows the integration of all components of the network to be tracked in real time.

A key success factor in implementing a CMDB is the ability to automatically discover and track real-time changes to the system components. For many designs, this stops at a logical view of the network. Only seeing the interconnection of network equipment as objects does not provide true situational awareness of the network. A system that shows the equipment tied to real space and to see and respond to real-time changes is needed.

Real-time Infrastructure Management (RTIM) is a strong answer to a lack of situational awareness. RTIM provides a physical layer, structured cabling system view of the network and components. From the work area equipment to the server, all of the cabling is tracked in real time, capturing new installs and moves, adds and changes. Without RTIM at the physical layer, even the best integrated systems have a huge blind spot in their CMDBs. Similar to an anchor chain holding a ship in place, the communications infrastructure is secured by the structured cabling system. Without RTIM, those components cannot be tracked.

RTIM improves the efficiency and accuracy of network provisioning, reduces network operations costs and enhances the mission readiness of the network, while detecting and physically locating network intrusions. RTIM is applicable to both the Network Defense (NetD) and Network Support (NS) operational activities of the military's Network Warfare Operations mission.

With RTIM, operational control of the network physical layer can be maintained, ensuring that time sensitive and/or mission-critical applications are allocated necessary physical bandwidth to meet mission objectives. In addition, RTIM enables unauthorized or suspicious network connections to be identified, physically located and countered. It provides network operators and users the confidence that their network infrastructure is properly configured, reliable and secure.

Without intelligent infrastructure solutions, critical physical links within the network cannot be monitored or managed in real time. Using traditional methods, the integrity of cabling (copper or fiber) connections and the security of the information channels can only be verified by time-consuming manual methods. Consequently, network connections can be inadvertently or surreptitiously disconnected causing the organization to lose vital connectivity for hours while the problem is manually traced. Furthermore, unauthorized connections to the network can present a security risk that may take hours or days to locate and address.

RTIM provides an immediate alarm that alerts the network operator to the presence and physical location of unauthorized changes to network connectivity. Additionally, RTIM can automatically initiate a variety of countermeasures or mitigation activities to address the unauthorized access.

RTIM enables planning and management of network connectivity changes (moves, adds and changes) that are normally tedious, paper-based processes. As the changes are recorded by the system in real time, there is no chance that the recording of the change will be missed.

CommScope's SYSTIMAX® iPatch® Intelligent Infrastructure Solutions (IIS) is one system that addresses the needs of RTIM. It uses a fully integrated software and hardware solution to secure the network physical layer, while enabling near real-time situational awareness for network management, provisioning and physical mapping of network connections. It enables direct access, control and monitoring of vital physical layer channel connections within the network from a central network operations center, remote terminal or locally within the facility.

The SYSTIMAX iPatch IIS provides an intelligent, real-time infrastructure management solution comprising intelligent copper and fiber patch panels, a Rack Manager Plus unit for managing and monitoring the panels in a rack or cabinet and System Manager Software. In a Department of Defense communications network, it would simplify the management and control of the physical interconnections between the network elements.

For an organization's CMDB to give an accurate real-time picture of the capability and availability of the network, the structured cabling component cannot be overlooked. Without RTIM, a critical component to federally mandated ITIL frameworks is overlooked. If the components' CMDBs don't address structured cabling, they are missing a primary anchoring component, allowing weak-link into the ITIL and CMDB chain. In a truly federated design, the effect of this weak-link could multiply across multiple organizations.

Without RTIM providing situational awareness, the most sophisticated Network Centric Warfare (NCW) platforms are rendered blind at the Physical Layer. For systems dependent upon real-time situational awareness, this remains a critical flaw. The network needs to always be ready to deliver up-to-date and accurate data to the warfighter. Delays in service provisioning, security breaches and network availability cannot impact the mission. RTIM offers significant enhancement to an organization to assure information assurance. By providing physical layer situational awareness to the IT team, intelligence personnel are better equipped to support the warfighter in the battle space.



Kevin Gleason
Technical Manager
CommScope Government Solutions

As Technical Manager for the federal government business unit of CommScope, he works with customers, consultants and business partners on communications infrastructure solutions for U.S. government agencies/departments and the U.S. military both in CONUS and OCONUS. Prior to joining CommScope, he was part of the AVAYA Architect, Consultant, Engineering (ACE) Team that helped the ACE community with technical issues as well as in the writing of specification language and documents. He has over 20 years experience in the design, installation and troubleshooting communications infrastructure. Kevin has extensive experience in a variety of optical and copper based technologies, systems acquisition and U.S. government operational requirements.

